Claims

1. A computer-implemented method for computer virus prevention, said method comprising the steps of:

entering a first computer virus status mode in response to a first computer virus outbreak report;

generating a first computer virus alert time corresponding to entry into the first computer virus status mode;

comparing a time stamp of a computer content with the first computer virus alert time; and

determining the executability of the computer content in response to the result of the comparing step.

2. The method of claim 1, wherein the step of generating the first virus alert time comprises the steps of:

entering a first access control time based on the first virus outbreak report; and

converting the first access control time into the first virus alert time.

3. The method of claim 2, wherein the first access control time is a relative time stamp.

4. The method of claim 2, wherein the first access control time is a pre-determined time period for access control under the first computer virus status mode.

5. The method of claim 1, further comprising the step of:

determining the presence of a value representing the computer content in a memory table of executable computer content.

6. The method of claim 5, wherein the computer content is not executed when the value representing the computer content is not present in the memory table of executable computer content.

7. The method of claim 5, wherein the value is a hash value of the computer content.

8. The method of claim 1, wherein the computer content is executed only when the computer content is time stamped prior to the first computer virus alert time.

9. The method of claim 1, further comprising the steps of:

entering types of computer codes that should be blocked from execution in response to the first computer virus outbreak report; and

blocking execution of a computer code that belongs to the entered types of computer codes.

10. The method of claim 1, further comprising the steps of:

generating a second virus alert time in response to a second computer virus outbreak report;

comparing the time stamp of the computer content with the second computer virus alert time;

performing anti-virus processing upon the computer content; and

determining the executability of the computer content in response to the result of comparing the time stamp of the computer content with the second computer virus alert time.

11. The method of claim 1, wherein the computer content is attached to an E-mail body, and said method further comprises the steps of:

removing the computer content from the E-mail body; and

denying execution of the computer content.

12. A computer access control system for computer virus prevention, said system comprising:

an access control console, for entering a first computer virus status mode and for generating a virus access control time; and

an anti-virus module, coupled to the access control console, configured to generate a virus alert time based on the virus access control time and to compare a time stamp of a target computer content with the virus alert time prior to execution of the target computer content.

13. The system of claim 12, wherein the target computer content is one of a plurality of computer contents, and the anti-virus module further comprises:

a memory module for storing time stamps of the plurality of computer contents; and

an access control module, coupled to the access control console and to the memory module, for generating the virus alert time and for comparing the time stamp of each target computer content with the virus alert time.

14. The system of claim 13, wherein the anti-virus module further comprises:

a computer virus processing module, coupled to the access control module, for further processing a target computer content in order to determine the executability of the target computer content.

15. The system of claim 13, wherein the memory module stores a value representing each of the computer contents.

16. The system of claim 15, wherein the access control module is configured to determine the presence of the value in the memory module as representing a target computer content.

17. The system of claim 15, wherein the value is a hash value.

18. An anti-virus module, comprising:

a memory module for storing time stamps of computer contents; and

an access control module, coupled to the memory module, for comparing the time stamp of a computer content with a computer virus alert time to determine the executability of the computer content.

19. The anti-virus module of claim 18, further comprising:

a computer virus processing module, coupled to the access control module, for further processing the computer content.

20. A computer-implemented method for computer virus prevention, said method comprising the steps of:

creating a list of time-stamped executable computer contents;

entering a virus alert mode in response to a virus outbreak report;

responsive to the virus alert mode, entering an access control message for specifying an access control rule for blocking the execution of suspicious or susceptible computer contents that are time-stamped not before a virus alert time, the access control message including a first control parameter for generating the virus alert time;

receiving a request to execute a target computer content; and

determining the executability of the target computer content based on the access control rule in the access control message.

21. The method of claim 20, wherein the step of creating a list of time-stamped executable computer contents, comprises:

applying anti-virus operation upon each executable computer content;

storing a hash value of each executable computer contents in the list; and

inserting a time stamp corresponding to the moment of storing the hash value of the executable computer content.

22. The method of claim 20, wherein the step of determining the executability of the target computer content comprises the steps of:

receiving the access control message;

converting the first control parameter into the virus alert time;

comparing the time stamp of the target computer content in the list with the virus alert time; and

determining the executability of the target computer content based on the result of the comparing step.

23. The method of claim 22, further comprising the step of:

applying an anti-virus operation upon the target computer content.

24. The method of claim 20, wherein the control message comprises:

a second control parameter for specifying types of computer contents that should be subject to the access control rule;

a third control parameter for specifying an expiration time for the access control rule; and

a fourth control parameter for identifying the access control message.

25. The method of claim 24, further comprising the step of:

determining validity of the access control message based on the third control parameter.

26. The method of claim 24, further comprising the step of:

determining executability of the target computer content based on the second control parameter.

27. A computer-implemented method for computer virus prevention, said method comprising the steps of:

creating a list of time-stamped executable computer contents;

entering a virus alert mode in response to a virus outbreak report;

responsive to the virus alert mode, entering an access control message for specifying an access control rule for blocking data communication initiated by computer contents that are time-stamped not before a virus alert time, the access control message including a first control parameter for generating the virus alert time;

receiving a request to examine a target computer content that participates in the data communication; and

determining whether the data communication should be blocked based on the access control rule.

28. The method of claim 27, wherein the step of determining whether the data communication should be blocked comprises the steps of:

receiving the access control message;

converting the first control parameter into the virus alert time;

comparing the time stamp of the target computer content in the list with the virus alert time; and

determining whether the data communication should be blocked based on the comparing step.

29. The method of claim 28, wherein the data communication is blocked when the target computer content is time-stamped not before the virus alert time.

30. A computer access control system for computer virus prevention, comprising:

a firewall module monitoring data communications initiated by a target computer content and sending a request to examine the data communications;

an access control console, for generating an access control message specifying an access control rule for blocking data communications of the target computer contents that are time-stamped not before a virus alert time, the access control message including a first control parameter for generating the virus alert time; and

an access control module, coupled to the access control console and the firewall module, configured to receive the access control message and a request from the firewall module, and to generate the virus alert time based on the virus access control time and to determine whether the data communication should be blocked based on the access control rule.

31. A computer program product comprising:

a computer usable medium having computer readable code embodied therein for computer access control for computer virus prevention, the computer program product comprising:

a computer readable program code device configured to receive a computer virus status mode in response to a computer virus outbreak report;

a computer readable program code device configured to generate a computer virus alert time corresponding to entry into the computer virus status mode;

a computer readable program code device configured to compare a time stamp of a computer content with the computer virus alert time; and

a computer readable program code device configured to determine executability of the computer content in response to the result of comparing the time stamp of the computer content with the computer virus alert time.

32. A computer access control system for computer virus prevention, said system comprising:

means for entering a computer virus status mode and for generating a virus access control time; and

coupled to the entering and generating means, means for calculating a virus alert time based on the virus access control time; and

coupled to the calculating virus alert time means, means for comparing a time stamp of a target computer content with the virus alert time prior to execution of the computer content.

33. A computer access control system for computer virus prevention, said system comprising:

means for storing time-stamped executable computer contents;

a firewall means for monitoring data communications occurring to the executable computer contents;

means for entering a computer virus status mode and for generating a virus access control time;

coupled to the entering and generating means, means for calculating a virus alert time based on the virus access control time; and

coupled to the calculating virus alert time means and the storing means and the firewall means, means for comparing a time stamp of an executable computer content with the virus alert time to determine whether the data communication occurring to the executable computer content should be blocked .